Yoga Pratama

Bunga Rampai

Pemikiran HUKUM INTERNASIONAL

Muhamad Nafi Uz Zaman

BAB VI

SERANGAN RANSOMWARE DAN PERETASAN TERHADAP PENERBANGAN SIPIL DALAM PERSPEKTIF HUKUM UDARA INTERNASIONAL

Adya Paramita Prabandari, Zahra Nur Aliya,
Pulung Widhi Hari Hananto

A. Pendahuluan

Tatanan dunia telah berubah dengan sangat cepat semenjak terjadinya Revolusi 3T.[136] Revolusi 3T merupakan revolusi yang memuat tiga bidang, yakni transportasi, telekomunikasi, dan travel. Mengutip pernyataan Dorodjatun Kuntjoro Jakti, bahwa revolusi ini telah menciptakan ruang mobilitas bagi barang, jasa, uang dan modal, teknologi, informasi, maupun mobilitas

136 Prabandari, A. P., Susetyorini, P., & Hartono, D. The Urgency of Ratification of the 2010 Beijing Convention Concerning Enforcement of Unlawful Acts Against International Civil Aviation. *Academic Journal of Interdisciplinary Studies*, Vol. *9*(2), (2020), hlm. 31–35.

penduduk.[137] Revolusi ini telah berlangsung sejak awal abad 21 dan dikenal dengan globalisasi.[138] *International Monetary Fund* (IMF) pun menyebutkan dalam penelitiannya bahwa globalisasi berperan dalam perkembangan teknologi informasi lintas batas.[139]

Perkembangan teknologi informasi lintas batas ini dapat terjadi karena adanya internet, yang memungkinkan pengguna untuk berkomunikasi dan bertukar data melalui jaringan server komputer.[140] Saat ini, internet telah menjadi hal yang tidak dapat dipisahkan dalam kehidupan masyarakat sehari-hari karena banyak sektor yang mengintegrasikan dengan internet, salah satunya yaitu sektor transportasi udara.

Transportasi udara merupakan satu-satunya jaringan transportasi cepat di seluruh dunia sehingga penting untuk bisnis global di mana berperan memfasilitasi perdagangan internasional dan pariwisata. Ketersediaan layanan transportasi udara yang andal pun memberikan akses pada hal-hal yang dibutuhkan oleh masyarakat, seperti akses pelayanan kesehatan dan pendidikan. Data dari *International Civil Aviation Organization* (ICAO) pun menyebutkan bahwa pada tahun 2018 terdapat 4,3 miliar penumpang yang mana diperkirakan akan tumbuh menjadi sekitar sepuluh miliar penumpang pada 2040.[141] Hal ini menunjukkan banyak orang yang mengandalkan transportasi udara.

> Industri transportasi udara atau penerbangan mencakup hampir semua aspek perjalanan udara dan kegiatan yang membantu memfasilitasinya. Secara singkat, industri

137 Jakti, D. K. *Perencanaan Ekonomi Nasional Menghadapi Tantangan Globalisasi*. Jakarta: Gramedia Pustaka Utama, 1995.

138 Prabandari, AP. *Op.cit.*

139 Aslam, A., Eugster, J., Ho Giang, Jaumotte, F., & Piazza, R. (2018, April 9). Globalization Help Spread Knowledge and Technology Across Borders.

140 Küenzl, J., Schwabenland, C., Elmaco, J., Hale, S., Levi, E., Chen, M., … Levi, E. (2010). Information Technology/Internet. In *International Encyclopedia of Civil Society* (pp. 853–858). New York, NY: Springer US. https://doi.org/10.1007/978-0-387-93996-4_555

141 We Forum. (2023, August 5). Cybersecurity in Aviation: Building A Resilient Future.

ini mencakup pesawat terbang, maskapai penerbangan dan bandara. Dalam rangka meningkatkan layanan penerbangan kepada penumpang, maskapai penerbangan dan bandara pun mengintegrasikan dengan internet. Sebagai contoh, penggunaan *boarding pass* elektronik di bandara. Penggunaan *boarding pass* elektronik ini memungkinkan penumpang untuk melewati pemeriksaan keamanan dengan menggunakan kode *Quick Response* (QR) dan *Short Message Service* (SMS) yang disediakan oleh maskapai penerbangan. Selain itu, penumpang pun juga dimudahkan untuk memilih tempat duduk dengan menggunakan akses internet.[142] Pengintegrasian internet pun juga diterapkan untuk mendukung ketahanan infrastruktur dan meminimalisir terjadinya kesalahan kecil atau kelalaian yang mengakibatkan berbagai kerusakan dan kerugian yang signifikan, misalnya, kematian, pencurian informasi data pelanggan, pencurian kredensial, dan hak kekayaan intelektual.[143]

Adanya pengintegrasian internet pada industri penerbangan ternyata memiliki resiko serangan siber, yaitu serangan *ransomware* dan peretasan. Menurut laporan yang dirilis oleh Eurocontrol (Eurocontrol adalah organisasi sipil militer Pan Eropa yang didedikasikan untuk mendukung penerbangan Eropa) pada Juli 2021 terjadi peningkatan serangan siber sebesar 530% dari tahun 2019-2020 dalam insiden yang dilaporkan di seluruh industri penerbangan dengan 61% serangan siber menargetkan maskapai penerbangan.[144] Data terbaru dari *European Union Agency*

142 Gou, L. Construction of Civil Aviation Airport Service Mode in Internet Plus Era. *Journal of Global Humanities and Social Sciences*, *3*(2), 2022, hlm. 19–20. https://doi.org/10.47852/ bonviewGHSS 2022030202

143 Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., … Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, *13*(3), 146. https://doi.org/10.3390/info13030146

144 Harwood, S. (2022, August 8). Aviation is facing a rising wave of cyber-attacks in

for Cyber Security (ENISA) menyebutkan bahwa ancaman paling tinggi pada Januari 2021-Oktober 2022 yakni berkaitan dengan data, disusul ancaman *ransomware* dan *malware*.[145].

ICAO sebagai organisasi penerbangan sipil internasional mulai merespon kejahatan berbasis internet ini dalam ruang lingkup keamanan siber *(cyber security)* sejak tahun 2000-an. Respon ini dapat dilihat dari *Standards and Recommended Practices* (SARPs), resolusi Majelis ICAO, dan instrumen hukum udara internasional yang dikeluarkan sebagai sarana menghadapi kejahatan berbasis internet terhadap penerbangan sipil.[146] Tetapi, dalam penerapannya terdapat tantangan digitalisasi infrastruktur secara historis. Fokus awal keamanan itu sendiri yakni keamanan fisik yang meliputi serangan kinetik terhadap pesawat terbang dan infrastruktur atau tindakan lain yang merupakan gangguan yang melanggar hukum terhadap operasi fisik penerbangan. Tetapi, kini telah bergeser ke jalinan dan virtualisasi infrastruktur siber dan fisik beserta resikonya.[147]

B. Permasalahan

Berdasarkan latar belakang yang telah diuraikan di atas, tulisan ini akan membahas dua rumusan masalah utama: 1) bagaimanakah kasus serangan *ransomware* dan peretasan yang menargetkan penerbangan sipil?; 2) bagaimanakah Hukum Udara Internasional merespon kasus serangan *ransomware* dan peretasan yang menargetkan penerbangan sipil?

---

the wake of COVID

145 Ćosić, J., & Mihailescu, M. I. (2023). *ENISA Threat Landscape: Transport Sector* . Attiki.

146 ICAO. (n.d.). Aviation Cybersecurity

147 Vedder, A. Safety, Security and Ethics. In *Security and Law* (pp. 11–26). Intersentia. 2019. https://doi.org/10.1017/9781780688909.002

C. Metode Penelitian

Metode penelitian yang digunakan yakni yuridis normatif, di mana hukum dikonsepkan sebagai apa yang tertulis dalam peraturan perundang-undangan *(law in books*).[148] Metode penelitian ini meletakkan hukum sebagai sebuah bangunan sistem norma. Sistem norma yang dimaksud yakni tentang asas, norma, kaidah dari peraturan perundangan, putusan pengadilan, perjanjian serta doktrin (ajaran).[149] Terdapat tiga pendekatan yang digunakan dalam penelitian ini. Pertama, yakni pendekatan perundang-undangan *(statute approach),* yang digunakan untuk menganalisis regulasi yang berkaitan dengan isu hukum yang dibahas. Kedua, menggunakan pendekatan konseptual *(conceptual approach)* untuk mengetahui makna yang termuat pada istilah-istilah hukum melalui analisis bahan hukum. Dalam rangka memvalidasi bahwa peristiwa kejahatan berbasis internet terhadap penerbangan sipil nyata terjadi, maka digunakan pula pendekatan kasus *(case approach)* untuk mendalami norma atau kaidah hukum yang dapat diaplikasikan dengan mengambil contoh kasus di masyarakat.[150]

Spesifikasi penelitian yang digunakan adalah deskriptif analitis. Penelitian hukum deskriptif analitis merupakan penelitian yang menggambarkan fakta-fakta yang terjadi dikaitkan dengan teori-teori hukum yang mendukung untuk menjawab permasalahan yang diteliti. Jenis data yang digunakan dalam penelitian ini yakni data sekunder. Data sekunder yang digunakan dalam penelitian ini dikumpulkan dengan penelusuran kepustakaan (*library research*). Metode analisis data yang digunakan dalam penelitian ini yakni analisis kualitatif.

148 Amiruddin and Z Asikin, *Pengantar Metode Penelitian Hukum* (Jakarta: Raja Grafindo, 2012).

149 ND, M. F., & Achmad, Y. (2022). *Dualisme Penelitian Hukum Normatif & Empiris* . Yogyakarta: Pustaka Pelajar.

150 Ibrahim, J. *Teori & Metodologi Penelitian Hukum Normatif* . Malang: Bayumedia Publishing, 2007.

D. Pembahasan

1. Kasus Serangan *Ransomware* dan Peretasan terhadap Penerbangan Sipil

Istilah penerbangan sipil dalam tulisan ini mengacu pada kategori operasi penerbangan yang bersifat non-militer, yang mencakup industri swasta dan komersial. Hal ini juga termasuk seluruh bagian ekosistem penerbangan, yang mencakup keseluruhan sistem avionik, pengatur lalu lintas udara, maskapai penerbangan, dan bandara. Berikut merupakan kasus serangan *ransomware* dan peretasan terhadap penerbangan sipil yang pernah terjadi:

a. Kasus Serangan *Ransomware* Terhadap Bandara Bristol

Pada September 2018, Bandara Bristol mengalami serangan *ransomware* yang menyebabkan layar tampilan informasi penerbangan mati selama dua hari. Tidak ada uang tebusan yang dibayarkan agar sistem dapat berfungsi kembali. Serangan ini tidak memengaruhi penerbangan maupun sistem keselamatan atau keamanan. Namun, proses manual seperti penggunaan papan tulis dan spidol sebagai pengganti layar informasi penerbangan dilakukan.[151] Pihak otoritas bandara mengatakan bahwa insiden tersebut terjadi karena infeksi *ransomware* sehingga informasi kedatangan dan keberangkatan bandara tidak dapat ditampilkan. Pihak bandara pun menghimbau penumpang untuk datang lebih awal dan memberikan waktu ekstra untuk proses *check-in.* Otoritas bandara mengatakan mereka tidak berniat membayar permintaan tebusan penyerang dan memilih untuk mematikan sistem mereka saat mereka memperbaiki komputer yang terkena dampak.[152]

151 BBC. (2018, September 16). Cyber attack led to Bristol Airport blank screens

152 Cimpanu, C. (2018, September 16). Ransomware attack blacks out screens at Bristol Airport.

b. Kasus Serangan *Ransomware* Terhadap Maskapai Penerbangan India SpiceJet

Pada Mei 2022, maskapai penerbangan India SpiceJet mengumumkan informasi kepada penumpang bahwa mereka mengalami serangan *ransomware* yang berdampak pada beberapa sistemnya dan penundaan keberangkatan penerbangan. Berdasarkan pengumuman yang dipublikasikan melalui media sosial maskapai tersebut, tim TI mereka berhasil menggagalkan serangan tersebut, sehingga status operasional kembali normal. Tetapi, masih terdapat beberapa laporan penumpang di media sosial yang menyoroti penundaan penerbangan, layanan pelanggan melalui telepon tidak dapat dihubungi, dan sistem pemesanan yang tidak tersedia.[153] Selain itu, penumpang pun mengatakan bahwa mereka menunggu berjam-jam tanpa makanan atau air.[154] SpiceJet merupakan maskapai penerbangan terbesar kedua di india dengan mengoperasikan sebanyak 102 pesawat untuk melayani lebih dari 60 tujuan. Perusahaan ini memiliki lebih dari 14.000 karyawan dan menguasai sekitar 15% pangsa pasar lokal. Oleh karenanya, serangan *ransomware* tersebut berdampak pada sejumlah besar penumpang di seluruh India dan tujuan internasional. Penundaan tersebut mengakibatkan kerugian finansial yang signifikan. SpijeJet sendiri mengatakan bahwa mereka juga menghubungi para ahli dan otoritas kejahatan dunia maya mengenai masalah ini.[155]

153 Toulas, B. (2022, May 25). SpiceJet airline passengers stranded after ransomware attack.

154 BBC. (2022, May 25). SpiceJet: Passengers stranded as India airline hit by ransomware attack.

155 Toulas, B. (2022, May 25). SpiceJet airline passengers stranded after ransomware attack

c. Kasus Peretasan *Vietnam Airlines* dan Bandara Vietnam

Pada Juli 2016, situs web sebuah maskapai penerbangan nasional *Vietnam Airlines* dan layar informasi penerbangan di dua bandara terbesar di Vietnam mengalami peretasan. Para peretas memasang pemberitahuan yang menurut media pemerintah mengecam Filipina dan Vietnam yang berselisih dengan Beijing mengenai kedaulatan maritim di Laut Cina Selatan. Selama beberapa menit juga terdapat pesan serupa diputar dan diucapkan oleh suara laki-laki dalam Bahasa Inggris.[156] Peretasan ini mengakibatkan penghentian *check-in* elektronik oleh operator bandara di Hanoi dan Ho Chi Minh. Media Vietnam menyebut peretasan itu diklaim oleh kelompok bernama 1937CN.[157] Tetapi, kelompok tersebut membantah keterlibatan mereka dalam serangan siber tersebut. Sementara itu, situs web *Vietnam Airlines* telah diambil alih, dipindahkan ke situs web jahat di luar negeri, dan dirusak untuk menampilkan peringatan serupa. Data penumpang mengenai sejumlah *frequent flyer* yang dirahasiakan juga dipublikasikan secara *online. Vietnam Airlines* meminta pelanggan *frequent flyer* untuk mengubah kata sandi mereka.[158]

Peretasan ini tidak berdampak pada keamanan *air traffic control* pada bandara. Pihak bandara pun telah mematikan layar dan sistem suara di Bandara Noi Bai di Hanoi dan Bandara Tan Son Nhat di Kota Ho Chi Minh.[159] Dalam merespon insiden tersebut, Pemerintah Vietnam meningkatkan Upaya untuk menghentikan insiden di

156 Davis, B. (2016, August 13). Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute.

157 The Guardian. (2016, July 29). Flight Information Screens in Two Vietnam Airports Hacked.

158 Blake, A. (2016, July 29). Cyberattack Claims Multiple Airports in Vietnam.

159 VOA. (2016, July 29). Flight Info Screens at Vietnam's Two Major Airports Hacked.

masa depan, tetapi respons komunitas teknologi lokal terhadap insiden tersebut harus dibatasi. Pemerintah mendesak komunitas teknologi Vietnam untuk tidak mengambil tindakan provokatif terhadap peretas asing. Di samping itu, komunitas teknologi Vietnam harus mematuhi hukum dan etika profesional.[160]

2. Serangan *Ransomware* dan Peretasan terhadap Penerbangan Sipil dalam Perspektif Hukum Udara Internasional

ICAO telah mengeluarkan sejumlah instrumen hukum udara internasional untuk mencegah terjadinya tindakan-tindakan yang mengancam keselamatan penerbangan sipil. Sebelum menyimpulkan mengenai keberlakuan instrumen hukum udara internasional yang ada saat ini untuk merespon serangan *ransomware* dan peretasan terhadap penerbangan sipil, penting untuk menganalisis muatan-muatan yang terdapat dalam instrumen-instrumen tersebut. Terdapat beberapa faktor yang berkontribusi menjadikan serangan *ransomware* dan peretasan sebagai sebuah peluang, seperti anonimitas, waktu serangan yang cepat, dan mekanisme serangan balik yang terbatas.[161] Sehingga, analisis instrumen hukum udara internasional dalam tulisan ini akan berfokus pada aktor atau pelaku yang diatur, tindakan-tindakan pelanggaran yang termuat dalam instrumen hukum udara internasional, dan yurisdiksi yang tercakup dalam instrumen hukum udara internasional.

a. Konvensi Chicago 1944

Konvensi Chicago 1944 menetapkan seperangkat aturan mengenai wilayah udara, pesawat terbang,

160 Thanh, V. Van, & Hai, V. (2016, August 2). Don't hack back: Vietnam's cyber community told to show restraint after attack.

161 Klenka, M. Aviation cyber security: legal aspects of cyber threats. *Journal of Transportation Security*, *14*(3–4), 2021, hlm. 177–195. https://doi.org/10.1007/s12198-021-00232-8

navigasi, registrasi, dan keselamatan. Melalui konvensi ini pula dibentuklah badan khusus PBB yang memiliki kewajiban mengoordinasi dan mengatur penerbangan sipil secara internasional (Klenka, 2021). Konvensi Chicago 1944 menyatakan bahwa konvensi tersebut hanya berlaku bagi pesawat udara sipil (*civil aircraft*) dan tidak berlaku bagi pesawat udara negara (*state aircraft*). Hal ini dinyatakan dalam Pasal 3(a) Konvensi Chicago 1944.

Konvensi Chicago 1944 mengalami amandemen penambahan setelah Pasal 3 yang tertulis sebagai *Article 3 bis* dalam *Protocol Relating to an Amendment to the Convention on International Civil Aviation* yang ditandatangani pada 10 Mei 1984 di Montreal. Sejarah dari Pasal 3 bis Konvensi Chicago 1944 dimulai sejak Perang Dunia I. Seperti yang diketahui, pada saat Perang Dunia I, pesawat banyak digunakan untuk tujuan militer dan tidak ada standar yang terkodifikasi..[162]

Pada tanggal 1 September 1982, pesawat sipil Korean Airlines Penerbangan 007 ditembak jatuh oleh Uni Soviet ketika memasuki wilayah udara Soviet.[163] Penembakan ini memicu gelombang kemarahan komunitas internasional dan berujung pada penerapan Pasal 3bis Konvensi Chicago 1944 yang melarang negara menggunakan kekerasan terhadap pesawat sipil.[164] Pada tanggal 10 Mei 1984, para anggota Majelis ICAO mengamandemen Konvensi Chicago 1944

162 Hartzenberg, B. *The Rights and Obligations of a State Under Article 3BIS of The Chicago Convention Purusant To An Intrusion of Its Sovereign Air Space by Civilian Aircraft (During Peace Time)*. University of Petroria, Petroria, 2019.

163 Laveson, J. D Korean Airline Flight 007: Stalemate in International Aviation Law – a Proposal for Enforcement. *The San Diego Law Review*, *22*(4), 1985, hlm. 859–894

164 Erotokritou, C. Sovereignity Over Airspace: International Law, Current Challenges, and Future Developments for Global Aviation. *Inquiries Journal*, *4*(5), 2012, hlm. 1–3.

sebagai reaksi terhadap jatuhnya Korean Airlines 007. Amandemen ini dilakukan dengan mengadopsi Pasal 3bis pada Konvensi Chicago yang melarang kekerasan terhadap pesawat sipil yang sedang terbang. Pasal 3bis baru berlaku pada tahun 1998 ketika Guinea dan Kuba meratifikasi amandemen tersebut.[165]

Berdasarkan Pasal 3bis, setiap negara harus menahan diri untuk tidak menggunakan senjata terhadap pesawat sipil yang sedang terbang. Selanjutnya, berdasarkan Pasal 3bis (b) apabila terdapat sebuah pesawat sipil yang mengganggu di atas wilayah suatu negara dapat dicegat dan diminta untuk mendarat di bandara yang ditentukan. Dalam merespon kasus serangan *ransomware* dan peretasan terhadap penerbangan sipil, kasus tersebut untuk dapat masuk dalam cakupan Pasal 3bis harus dianggap sebagai "senjata". Tetapi, istilah "senjata" tersebut tidak didefiniskan dalam Konvensi Chicago 1944 dan perlu dilakukannya interpretasi mengenai cakupan dari istilah "senjata" tersebut. Interpretasi atau penafsiran ini dapat merujuk pada Pasal 31 dan 32 *Vienna Convention on the Law of Treaties* (VCLT). Menurut Pasal 31 dan 32 VCLT terdapat beberapa prinsip penafsiran perjanjian internasional. Prinsip-prinsip tersebut di antaranya prinsip itikad baik (*good faith*), pengertian awal *(ordinary meaning)* terhadap suatu istilah dan konteksnya serta tujuan dari perjanjian internasional itu sendiri.[166]

b. Konvensi Tokyo 1963

Pada Pasal 1(1) Konvensi Tokyo 1963 menyebutkan bahwa konvensi ini berlaku untuk pelanggaran hukum pidana dan setiap tindakan yang mungkin atau memang

165 Hartzenberg, B. Op.cit.

166 Aprianto, A. Relevansi Monisme dan Dualisme Bagi Pemberlakuan Perjanjian Internasional di Indonesia. *Jurnal Konstitusi* , *19*(3), 2020, hlm. 580–605.

membahayakan keselamatan pesawat udara, orang atau harta benda di dalam pesawat, atau tindakan apa pun yang membahayakan ketertiban dan disiplin dalam pesawat (*on board*). Pada Pasal 3 Konvensi Tokyo 1963 memperjelas mengenai pemberian yurisdiksi kepada Negara Pendaftar (*state of registration*) atas pelanggaran yang dilakukan di dalam pesawat ketika penerbangan tersebut berada di atas wilayah internasional. Konvensi Tokyo 1963 berlaku apabila kejahatan berbasis internet dianggap sebagai tindakan yang merupakan pelanggaran secara langsung menurut hukum nasional atau berdasarkan penerapan hukum internasional, seperti Konvensi Budapest 2001. Selain itu, konvensi ini akan berlaku apabila kasus serangan *ransomware* dan peretasan mungkin atau memang membahayakan keselamatan pesawat, atau orang atau properti di dalamnya. Namun, konvensi ini memiliki limitasi yakni tidak ada rincian pelanggaran-pelanggaran yang dilakukan. Yurisdiksi yang diatur dalam konvensi ini pun dengan jelas menyebutkan bahwa yurisdiksi ada pada negara pendaftar (*state of registration*). Aktor dalam Konvensi Tokyo 1963 tidak disebutkan secara spesifik, sehingga berlaku bagi semua jenis aktor termasuk aktor non-negara dan individu.

c. Konvensi Den Haag 1970

Konvensi Den Haag 1970 diadopsi untuk memerangi pembajakan pesawat, Konvensi ini memuat ketentuan tentang kriminalisasi terhadap pelanggaran yang dilakukan di dalam pesawat udara yang sedang terbang. Konvensi Den Haag 1970 berfokus pada tindak pidana penguasaan pesawat udara secara melawan hukum dengan jalan kekerasan atau ancaman kekerasan. Pelanggaran tersebut berfokus ketika seseorang menyita atau menguasai pesawat udara tersebut. Dalam Pasal 1

pun tidak menyebutkan secara spesifik mengenai aktor hanya disebut sebagai "setiap orang".

Yurisdiksi pertama pada konvensi ini ditentukan oleh negara di mana pesawat udara mendarat dan adanya pembajak di dalam pesawat udara. Konvensi Den Haag 1970 pun dapat berlaku untuk kejahatan berbasis internet apabila penumpang melakukan serangan *ransomware* dan peretasan di dalam pesawat dengan tujuan mengambil kendali pesawat. Selain itu, kasus serangan *ransomware* dan peretasan perlu dianggap sebagai kekerasan *(by force)* yang dapat ditafsirkan secara berbeda tergantung pada yurisdiksi tempat kasus diadili.

d. Konvensi Montreal 1971

Konvensi Montreal 1971 menggunakan pendekatan berbasis dampak untuk menentukan pelanggaran, yang mempunyai kesamaan sebagai berikut: a. tindakan tersebut melanggar hukum; b. tindakan tersebut disengaja; dan c. tindakan tersebut kemungkinan membahayakan keselamatan pesawat dalam penerbangan. Konvensi Montreal 1971 tidak mewajibkan pelaku berada di dalam pesawat saat melakukan perbuatan melawan hukum. Selain itu, yurisdiksi yang diatur mencakup yurisdiksi atas pelanggaran yang dilakukan "terhadap atau di atas pesawat yang terdaftar di Negara tersebut." Hal ini secara efektif memperluas cakupan penerapan konvensi ini terhadap kasus serangan *ransomware* dan peretasan sebagai kejahatan siber yang dilakukan dari jarak jauh yang dapat berdampak tidak hanya pada pesawat terbang, tetapi juga fasilitas navigasi udara maupun penyedia informasi penerbangan penting yang dikirim ke pesawat. Konvensi Montreal 1971 tidak menyebutkan aktor secara spesifik, maka dapat dikatakan aktor yang tercakup dalam konvensi tersebut

yaitu semua jenis aktor termasuk aktor non negara dan individu. Pada Pasal 1(2) bahwa konvensi ini juga berlaku untuk tindakan percobaan dan kaki kanan *(accomplice)*.

Konvensi Montreal 1971 berfokus pada pencegahan dari tindakan-tindakan melawan hukum terhadap keselamatan penerbangan sipil. Berdasarkan Pasal 2(b), Konvensi ini memberikan perhatian bahwa tindakan-tindakan melawan hukum memungkinkan dilakukan pada saat pesawat sedang tidak dalam penerbangan, seperti pada saat lepas landas, pada saat pesawat masih berada di darat atau pada saat pesawat masih berada di suatu tempat di bumi.[167] Penjelasan mengenai yurisdiksi pada Konvensi Montreal 1971 diatur dalam Pasal 5(1) di mana negara-negara anggota diberikan panduan untuk menetapkan yurisdiksinya.

Konvensi Montreal 1971 selanjutnya mengalami amandemen melalui *Montreal Protocol 1988* (Protokol Montreal 1988). Amandemen ini dilakukan untuk memperluas penggaran dengan memasukkan tindakan kekerasan atau gangguan layanan di bandara internasional. Hal ini dijelaskan dalam Pasal 2 Protokol Montreal 1988.

Pada kasus kejahatan berbasis internet yang telah dipaparkan sebelumnya, terdapat dua kasus yang menargetkan bandara yaitu pada kasus serangan *ransomware* terhadap layar tampilan informasi penerbangan di Bandara Bristol dan peretasan layar informasi penerbangan di Bandara Hanoi dan Ho Chi Minh. Apabila mengacu pada Pasal 2 Protokol Montreal 1988, tiga kasus tersebut mungkin untuk masuk dalam

167 Manullang, Y. N., Widodo, H., & Angwarmasse, P. Y. Aspek Hukum Internasional Terhadap Yurisdiksi Dalam Mengadili Pelaku Pembajakan Pesawat Udara . *Jurnal Krisna Law*, 13, 2019, hlm. 109–128.

ruang lingkup Pasal 2 paragraf 1*bis* (b), tetapi karena tidak ada penafsiran mengenai istilah menghancurkan atau merusak parah, maka kasus tersebut pun belum tentu masuk dalam ruang lingkup Pasal 2 paragraf 1*bis* (b).

Pasal 2 paragraf 1*bis* (b) juga menyebut bahwa tindakan yang diatur dalam Pasal 2 paragraf 1*bis* (b) merupakan tindakan yang membahayakan atau memungkinkan membahayakan keselamatan di bandara tersebut. Sedangkan, dalam tiga kasus yang disebutkan dampak dari kejahatan berbasis internet tersebut, menurut hemat penulis tidak sampai pada kondisi membahayakan keselamatan di bandara tersebut. Hal ini dikarenakan dampak dari tiga kasus tersebut yaitu hanya disebutkan penundaan keberangkatan penerbangan.

e. Konvensi Beijing 2010

Konvensi Beijing 2010 dirancang untuk mengonsolidasikan ketentuan Konvensi Montreal 1971 dan Protokol Montreal 1988. Konvensi Beijing 2010 disusun setelah terjadinya penyerangan teroris terhadap *World Trade Centre* pada tanggal 11 September 2011. Konvensi Beijing 2010 memperluas cakupan perlindungan terhadap serangan terhadap layanan navigasi udara. Hal ini diperkenalkan dengan istilah fasilitas navigasi udara *(air navigation facilities)* berdasarkan Pasal 1(1) huruf d. Cakupan dari fasilitas navigasi udara tersebut menurut Pasal 2(c) yaitu sinyal, data, informasi atau sistem yang diperlukan untuk navigasi pesawat.

Definisi tersebut memberikan kejelasan lebih lanjut mengenai cakupan tindakan yang dapat mencakup serangan terhadap terhadap fasilitas dan pesawat tersebut dengan kejahatan berbasis internet. Konvensi Beijing 2010 tidak spesifik menyebutkan aktor, seperti

yang tertulis dalam Pasal 1 yaitu "setiap orang" *(any person)*. Konvensi ini berlaku untuk pelanggaran-pelanggaran yang dilakukan di dalam pesawat udara ketika pesawat udara tersebut sedang terbang atau di permukaan laut lepas atau di wilayah lain mana pun di luar wilayah suatu negara. Konvensi ini berlaku untuk tindakan yang mungkin atau memang membahayakan keselamatan pesawat udara atau ketertiban dan disiplin di dalam pesawat.

Yurisdiksi yang tercakup dalam Konvensi Beijing 2010 adalah negara tempat pendaftaran *(state of registration).* Pasal 4 Konvensi ini memberikan dasar-dasar lain, antara lain, pelanggaran tersebut dilakukan oleh atau terhadap warga negara atau penduduk tetap negara tersebut dan pelanggaran tersebut bertentangan dengan keamanan negara tersebut.

Terdapat beberapa tantangan dalam aplikasi Konvensi Beijing 2010, di antaranya: a) Serangan *ransomware* dan peretasan terhadap penerbangan sipil untuk dapat masuk ke dalam ruang lingkup Konvensi ini harus melihat apakah kejahatan berbasis internet tersebut merusak atau menyebabkan kerusakan pada pesawat terbang; b) Serangan *ransomware* dan peretasan harus diartikan sama dengan penempatan perangkat atau zat di dalam pesawat; c) Serangan *ransomware* dan peretasan harus dilihat apakah menghancurkan atau merusak fasilitas navigasi udara atau mengganggu pengoperasiannya dengan cara yang mungkin membahayakan keselamatan pesawat; d) Serangan *ransomware* dan peretasan harus melihat dampak dari penyampaian informasi palsu, apabila informasi palsu tersebut membahayakan keselamatan penerbangan, maka Konvensi Beijing 2010 pun berlaku; dan e) Serangan *ransomware* dan peretasan

yang menargetkan fasilitas bandara atau pesawat udara haruslah membahayakan keselamatan.

f. Protokol Beijing 2010

Protokol ini mendefinisikan kembali pengertian pesawat dalam pelayanan *(in service)* dalam Pasal 5-nya. Pesawat dalam pelayanan *(in service)* diartikan sebagai dari awal persiapan pra penerbangan pesawat hingga dua puluh empat jam setelah pendaratan. Jangka waktu yang lebih luas ini relevan dengan skenario di mana serangan *ransomware* dan peretasan dilakukan selama persiapan penting sebelum penerbangan, seperti penghitungan dan dokumentasi penerbangan yang relevan dengan keselamatan atau skenario kejahatan berbasis internet yang terjadi selama fase pasca-penerbangan yang ditentukan, seperti aktivitas pemeliharaan tertentu.

Terdapat dua dasar tambahan yurisdiksi yang dimasukkan dalam Protokol Beijing pada Pasal 7 yaitu ketika pelanggaran dilakukan di wilayah Negara tersebut atau ketika dilakukan oleh warga negara dari Negara tersebut. Dua dasar opsional juga disertakan, ketika pelanggaran tersebut dilakukan. terhadap warga negara atau orang tanpa kewarganegaraan yang biasa tinggal di Negara tersebut. Pasal 3 protokol ini mewajibkan Negara untuk menjatuhkan hukuman yang berat atas pelanggaran yang dilakukan.

g. *Annex 17* Konvensi Chicago 1944

Annex 17 Konvensi Chicago 1944 tentang *Safeguarding International Civil Aviation Against Acts of Unlawful Interference* diadopsi oleh ICAO pada tahun 1974 yang memuat keamanan penerbangan. *Annex* ini mensyaratkan bahwa setiap negara anggota mempunyai tujuan utama untuk keselamatan penumpang, awak kapal, personel darat dan masyarakat umum dalam

segala hal yang berkaitan dengan perlindungan terhadap tindakan campur tangan yang melanggar hukum terhadap penerbangan sipil. Pada awal tahun 1970-an, ICAO menerbitkan *Aviation Security Manual* 43 untuk membantu Negara-negara Anggotanya mengambil tindakan untuk mencegah campur tangan yang melanggar hukum, meminimalkan dampaknya, dan menetapkan standar dengan mengadopsi *Annex 17 Chicago Convention*, sehingga membangun budaya keamanan. Namun, ancaman yang ditimbulkan oleh keamanan siber masih belum ditangani hingga saat ini. ICAO tampaknya berasumsi bahwa karena telekomunikasi adalah subjek nasional, masing-masing negara menentukan apa yang melewati wilayahnya dan tanggung jawab atas kekurangan keamanan berada di tangan negara tersebut. Tetapi, ancaman di dunia dimana lalu lintas, data, suara, video, dll ditransmisikan melalui Internet, sikap ini tidak dapat dipertahankan dalam jangka Panjang (Klenka, 2021).

Pada tanggal 21 hingga 26 Maret 2010 terdapat amandemen *Annex 12* di mana terdapat usulan mengenai praktik baru yang direkomendasikan terkait dengan ancaman siber. Rekomendasi ini kemudian diadopsi pada 17 November 2010 dan berlaku efektif pada 26 Maret 2011. Praktik yang direkomendasikan ini menyarankan agar setiap negara anggota mengembangkan langkah-langkah untuk melindungi sistem teknologi informasi dan komunikasi yang digunakan untuk tujuan penerbangan sipil dari gangguan. yang dapat membahayakan keselamatan penerbangan sipil. Pada Pertemuan Panel ke-22, yang diadakan oleh ICAO pada tanggal 21 hingga 25 Maret 2011, Panel mencatat nilai penilaian kerentanan yang berkaitan dengan keamanan siber dalam penerbangan yang bertujuan untuk mengevaluasi efisiensi langkah-

langkah mitigasi yang ada dan mengidentifikasi kerentanan apa pun dari perspektif berbasis ancaman. Lebih lanjut dicatat bahwa pemahaman yang lebih baik mengenai resiko akan mendukung upaya suatu negara untuk menyempurnakan respons resikonya.[168]

Dalam *Annex 17, Standard 4.9.1* (langkah-langkah yang berkaitan dengan ancaman dunia maya) telah diperkenalkan, yang mengharuskan negara untuk mengembangkan dan menerapkan langkah-langkah untuk melindungi informasi penting, sistem teknologi komunikasi, serta data yang digunakan untuk tujuan penerbangan sipil dari campur tangan yang melanggar hukum.

Sektor penerbangan masih berupaya memahami ancaman, resiko, dan manajemen keamanan siber. Berbagai badan dan organisasi seperti *Aviation Information Sharing and Analysis Center (ISAC), International Aviation Transport Association,* dan ICAO telah memberikan pedoman dan instruksi tentang resiko yang akan muncul. Keamanan siber pada penerbangan sipil memiliki dua aspek penting yakni keselamatan (*safety*) dan keamanan (*security*) Regulasi mengenai keselamatan dan keamanan didesain untuk menghindari kerusakan pada orang dan properti.[169] Dapat dikatakan bahwa keselamatan juga termasuk keamanan. Keamanan berarti menjaga penerbangan sipil dari tindakan atau upaya yang membahayakan keselamatan penerbangan sipil,[170] seperti pembajakan, perusakan pada pesawat udara

168 R Abeyratne, "Cyber Terrorism and Aviation—National and International Responses," *Journal of Transportation Security* 4, no. 4 (2011): 337–349, https://doi.org/10.1007/s12198-011-0074-3.

169 Dempsey, P. Stephen., Milde, M. (Lawyer), & McGill University. Institute of Air and Space Law. (2008). *Public International Air Law*. 463. Retrieved from https://papers.ssrn.com/abstract=3295922

170 Huang, Jiefang. *Aviation safety and ICAO*. Kluwer Law International, 2009, Retrieved from https://hdl.handle.net/1887/13688

atau penyampaian informasi palsu yang membahayakan keselamatan pesawat udara dalam penerbangan, di darat, penumpang, awak kapal, personel darat atau masyarakat umum, di bandara atau lokasi fasilitas penerbangan sipil.[171]

Upaya untuk mencapai keselamatan dapat dicapai melalui keseragaman dan dengan menjaga keselarasan hukum bersama. Menurut Michael Milde, penerbangan sipil tidak akan berkembang tanpa keseragaman peraturan di seluruh dunia, hal ini meliputi standar dan prosedur yang berkaitan dengan navigasi udara (Milde, 2008). Keseragaman tersebut tercapai ketika negara-negara anggota Konvensi Chicago terikat dengan perjanjian dan pada saat ICAO menentukan SARPs.

Negara memang memiliki kewajiban di bawah Konvensi Chicago untuk menjaga keseragaman peraturan mereka semaksimal mungkin dengan SARP, tetapi konvensi dirancang memberikan negara peserta suatu cara untuk menghindari penerapan standar atas dasar ketidakpraktisan. Hal ini diatur dalam Pasal 38 Konvensi Chicago 1944. Oleh karena itu, beberapa negara mungkin menganggap tidak praktis untuk mematuhi didasarkan pada kondisi kurangnya sumber daya manusia atau keuangan atau keunikan geografis atau karakteristik teknologinya. Atas keadaan/kondisi tersebut, negara memiliki kewajiban untuk segera memberi tahu/menginformasikan kepada ICAO mengenai perbedaan antara praktik mereka dengan apa yang sudah diatur oleh standar internasional (Iannini, 2016).

Meskipun negara-negara anggota memiliki hak untuk membatasi pesawat terbang tertentu di udara, mereka tidak bisa/tidak memiliki hak untuk mengabaikan mandat keselamatan ICAO. Asumsi kepatuhan universal ini sejalan dengan persyaratan Konvensi Chicago bahwa sertifikat

171 Iannini, M. C. *Civil Aviation and Cybersecurity: New Challenges*. McGill University, Montreal, 2016.

penerbang atau operator atau sertifikat kelaikan udara yang diterbitkan dengan benar oleh satu negara anggota akan diakui sebagai sah oleh negara lain.[172] Prinsip pengakuan timbal balik tersebut hanya akan berhasil jika semua negara menerapkan SARPs dengan tingkat ketekunan yang setara atau lebih tinggi yang disyaratkan berdasarkan *annexes*. Meskipun ICAO telah berupaya memfasilitasi kepatuhan dengan menerbitkan berbagai manual yang menginstruksikan negara anggota untuk mematuhi, banyak negara anggota yang tidak bisa atau tidak akan mengimplementasikan kewajiban keselamatan yang telah ditetapkan oleh instrumen hukum internasional.

Amerika Serikat melalui *Federal Aviation Administration* (FAA) dan Uni Eropa melalui *European Aviation Safety Agency* (EASA), telah mengembangan mekanisme tambahan untuk mengimplementasikan prosedur keselamatan dan kemanan. Sebagai contoh, pemerintah Amerika Serikat menerapkan prosedur keamanan tambahan untuk bandara asing dan maskapai penerbangan asing yang melayani Amerika Serikat melalui *Foreign Air Security Act 1985*. Bandara asing dinilai oleh *Department of Transportation* (DOT) untuk menentukan apakah mereka memenuhi persyaratan yang ditetapkan oleh ICAO berdasarkan *Annex 17* yang mengatur mengenai keamanan.[173]

DOT melakukan audit keamanan pada bandara asing dan apabila menemukan bahwa bandara gagal untuk mengambil langkah-langkah keamanan yang tepat, akan memberi tahu otoritas yang berwenang, merekomendasikan langkah-langkah untuk mencapai kepatuhan dan sertifikasi atau mencabut sertifikat bandara asing yang didasarkan pada hasil audit keamanan.[174] Beberapa bandara di dunia

172 Iannini M, C. *Op.cit*.

173 Iannini M, C. *Op.cit*.

174 Iannini M, C. *Op.cit*.

yang telah bersertifikat dan lalu dicabut sertifikatnya oleh DOT yaitu Murtala Mohammed International Airport di Lagos, Nigeria, El Dorado International Airport di Bogotá, Colombia dan Hellenikon International Airport di Athens, Greece.

Beberapa perjanjian yang mengatur mengenai keamanan penerbangan merupakan instrumen hukum yang berguna untuk melawan tindakan melawan hukum terhadap penerbangan sipil. Namun, dengan berjalannya waktu dan kondisi yang berubah, terdapat pengembangan baru yang juga menjadikan ancaman terhadap penerbangan sipil. Ancaman tersebut tidak diatur dalam perjanjian-perjanjian yang sudah ada karena perjanjian yang ada hanya mengkriminalisasi beberapa pelanggaran. Serangan ransomware dan peretasan dapat menjadi ancaman yang mencakup keselamatan dan keamanan di mana tidak ada perjanjian-perjanjian/instrumen hukum udara internasional mengaturnya secara komprehensif.

Serangan *ransomware* dan peretasan sebagai akibat dari perkembangan teknologi, informasi dan globalisasi memungkinkan menjadi kejahatan transnasional yang terus berkembang. Pada masa depan tidak menutup kemungkinan serangan *ransomware* dan peretasan terhadap penerbangan sipil dilakukan oleh kelompok kejahatan terorganisir dan berdampak pada seluruh masyarakat dunia. Tidak ada instrumen internasional yang mengatur mengenai yurisdiksi di ruang siber yang dapat digunakan untuk merespon serangan *ransomware* dan peretasan di mana pelaku dan korban tidak berada dalam yurisdiksi yang sama.[175] Penerbangan sipil pun menjadi sektor yang terdampak dalam kompleksitas yurisdiksi kejahatan siber sebagai kejahatan transnasional.

175 Rawat, M. Transnational Cybercrime: Issue of Jurisdiction. *International Journal of Law Management & Humanities*, *4*(2), 2021, hlm. 253–266.

E. Penutup

1. Kesimpulan

Pengintegrasian internet terhadap penerbangan sipil berpotensi menimbulkan ancaman terhadap penerbangan sipil, seperti ancaman serangan *ransomware* dan peretasan. Serangan *ransomware* dan peretasan tersebut menargetkan maskapai penerbangan dan bandara. Instrumen aturan yang telah tersedia masih belum cukup untuk merespon serangan *ransomware* dan peretasan dalam penerbangan sipil, Serangan *ransomware* dan peretasan dilakukan dari jarak jauh dan penilaian dampak dari serangan tersebut masih perlu diidentifikasi. Hal ini dikarenakan instrumen hukum udara internasional yang tersedia mensyaratkan pelanggaran membahayakan keselamatan penerbangan. Penyeragaman aturan mengenai penerbangan sipil pun belum maksimal, negara anggota memiliki kewajiban di bawah Konvensi Chicago 1944 untuk mematuhi standar minimum yang ditentukan oleh ICAO. Namun, negara anggota dapat memilih tidak mematuhi dengan alasan pengecualian yang dilegitimasi dalam Pasal 38 Konvensi Chicago 1944.

2. Saran

Berdasarkan analisis yang telah dilakukan, terdapat tiga saran yang penulis berikan, yaitu:

a. Pembentukan Mahkamah Penerbangan diperlukan untuk mengadili kejahatan berbasis internet terhadap penerbangan sipil yang diharapkan dapat mengurangi impunitas pelaku kejahatan penerbangan, terkhusus kejahatan berbasis internet;

b. Negara anggota, penyedia layanan penerbangan, otoritas penerbangan sipil, organisasi regional, maupun ICAO harus aktif dalam bertukar informasi maupun mengenai keamanan siber dalam penerbangan sipil;

c. ICAO dapat proaktif mendorong negara anggota untuk patuh pada instrumen hukum udara internasional yang mana dapat merujuk pada proses audit DOT AS;
d. Pengembangan kapasitas bagi pilot dan awak pesawat mengenai keamanan siber dan ancaman kejahatan berbasis internet.

Daftar Pustaka

Abeyratne, R. (2011). Cyber terrorism and aviation—national and international responses. *Journal of Transportation Security*, *4*(4), 337–349. https://doi.org/10.1007/s12198-011-0074-3

Amiruddin, & Asikin, Z. (2012). *Pengantar Metode Penelitian Hukum* . Jakarta: Raja Grafindo Persada .

Aprianto, A. (2022). Relevansi Monisme dan Dualisme Bagi Pemberlakuan Perjanjian Internasional di Indonesia. *Jurnal Konstitusi* , *19*(3), 580–605.

Aslam, A., Eugster, J., Ho Giang, Jaumotte, F., & Piazza, R. (2018, April 9). Globalization Help Spread Knowledge and Technology Across Borders.

BBC. (2018, September 16). Cyber attack led to Bristol Airport blank screens.

BBC. (2022, May 25). SpiceJet: Passengers stranded as India airline hit by ransomware attack.

Blake, A. (2016, July 29). Cyberattack Claims Multiple Airports in Vietnam.

Cimpanu, C. (2018, September 16). Ransomware attack blacks out screens at Bristol Airport.

Ćosić, J., & Mihailescu, M. I. (2023). *ENISA Threat Landscape: Transport Sector* . Attiki.

Davis, B. (2016, August 13). Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute.

Dempsey, P. Stephen., Milde, M. (Lawyer), & McGill University. Institute of Air and Space Law. (2008). *Public International Air Law*. 463. Retrieved from https://papers.ssrn.com/abstract=3295922

Erotokritou, C. (2012). Sovereignity Over Airspace: International Law, Current Challenges, and Future Developments for Global Aviation. *Inquiries Journal*, *4*(5), 1–3.

Gou, L. (2022). Construction of Civil Aviation Airport Service Mode in Internet Plus Era. *Journal of Global Humanities and Social Sciences*, *3*(2), 19–20. https://doi.org/10.47852/bonviewGHSS2022030202

Hartzenberg, B. (2019). *The Rights and Obligations of a State Under Article 3BIS of The Chicago Convention Purusant To An Intrusion of Its Sovereign Air Space by Civilian Aircraft (During Peace Time)*. University of Petroria , Petroria .

Harwood, S. (2022, August 8). Aviation is facing a rising wave of cyber-attacks in the wake of COVID.

Huang, Jiefang. (2009). *Aviation safety and ICAO*. Kluwer Law International. Retrieved from https://hdl.handle.net/1887/13688

Iannini, M. C. (2016). *Civil Aviation and Cybersecurity: New Challenges*. McGill University, Montreal .

Ibrahim, J. (2007). *Teori & Metodologi Penelitian Hukum Normatif* . Malang: Bayumedia Publishing .

ICAO. (n.d.). Aviation Cybersecurity.

Jakti, D. K. (1995). *Perencanaan Ekonomi Nasional Menghadapi Tantangan Globalisasi*. Jakarta: Gramedia Pustaka Utama .

Klenka, M. (2021). Aviation cyber security: legal aspects of cyber threats. *Journal of Transportation Security*, *14*(3–4), 177–195. https://doi.org/10.1007/s12198-021-00232-8

Küenzl, J., Schwabenland, C., Elmaco, J., Hale, S., Levi, E., Chen, M., … Levi, E. (2010). Information Technology/Internet. In *International Encyclopedia of Civil Society* (pp. 853–858). New York, NY: Springer US. https://doi.org/10.1007/978-0-387-93996-4_555

Laveson, J. D. (1985). Korean Airline Flight 007: Stalemate in International Aviation Law – a Proposal for Enforcement. *The San Diego Law Review*, *22*(4), 859–894.

Manullang, Y. N., Widodo, H., & Angwarmasse, P. Y. (2019). Aspek Hukum Internasional Terhadap Yurisdiksi Dalam Mengadili Pelaku Pembajakan Pesawat Udara . *Jurnal Krisna Law* , *13*, 109–128.

Milde, M. (2008). *Essential Air and Space Law: International Air Law and ICAO*. Den Haag: Eleven International Publishing .

ND, M. F., & Achmad, Y. (2022). *Dualisme Penelitian Hukum Normatif & Empiris* . Yogyakarta: Pustaka Pelajar.

Prabandari, A. P., Susetyorini, P., & Hartono, D. (2020). The Urgency of Ratification of the 2010 Beijing Convention Concerning Enforcement of Unlawful Acts Against International Civil Aviation. *Academic Journal of Interdisciplinary Studies*, *9*(2), 31–35.

Rawat, M. (2021). Transnational Cybercrime: Issue of Jurisdiction. *International Journal of Law Management & Humanities*, *4*(2), 253–266.

Thanh, V. Van, & Hai, V. (2016, August 2). Don’t hack back: Vietnam’s cyber community told to show restraint after attack.

The Guardian. (2016, July 29). Flight Information Screens in Two Vietnam Airports Hacked.

Toulas, B. (2022, May 25). SpiceJet airline passengers stranded after ransomware attack.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., … Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, *13*(3), 146. https://doi.org/10.3390/info13030146

Vedder, A. (2019). Safety, Security and Ethics. In *Security and Law* (pp. 11–26). Intersentia. https://doi.org/10.1017/9781780688909.002

VOA. (2016, July 29). Flight Info Screens at Vietnam's Two Major Airports Hacked.

We Forum. (2023, August 5). Cybersecurity in Aviation: Building A Resilient Future.